UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,018	11/12/2003	Xiaoxi Tan	MSFT-2737/304771.1	6192

41505 7590 12/10/2007

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
REZA, MOHAMMAD W	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
12/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/706,018	TAN ET AL.	
	Examiner	Art Unit	
	Mohammad W. Reza	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-22 and 24-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-22, and 24-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 09/19/2007.

2. Claims 1, 3-22, and 24-42 are pending in the application.

3. Claims 1, 3-22, and 24-42 have been rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1, 3-22, and 24-42 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Examiner failed to find any disclosure in any where in spec and figure that the obtained information being selected from a group consisting of a hardware identification (HWID) generated for the computing device based on one or more identifications of hardware of the computing device". The spec discloses that the computing devices generated the hardware id not the obtained information as amended in the claim (specification paragraphs, 0032).

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1, 3-22, and 24-42 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In these claims applicants mention "a number **x of locations** …. generating **x pseudo-random file names** and **x corresponding paths** based ….. pairing the x generated file names and the x generated paths to form the **x locations**; ……. **x generated locations**" which is generally narrative and indefinite with the invention. Applicants do not point out clearly which options include in the present invention by "**all these number of x**", and do not specifically mention what is the definite value included by x. It can be any value from zero to infinity and which is indefinite. Applicant also admitted in the argument (page 13) that x could be an indefinite number. Examiner could not understand how a claim could be still definite by using an indefinite term as applicant mentioned in his argument. The x number should be definite as it describing the locations, file and path. Examiner carefully reviewing the present specification and could not find any definite number regarding to the claim as it always mention in the indefinite way. Further, applicant claim language does not have any consistency in the steps, for example, "**determining** a number x of **locations**.....storing the state store according to the x **generated locations**." Examiner could not understand how **determined locations** and **generated locations** would be the same. Applicant determines the location not generates the location and at the end using the generated

location in stead of determined location is really confusing to understand. All these ambiguities arise because of using the indefinite number x. The office will interpret these words with the regarding claims as best understood for applying the appropriate art for rejection purposes.

6. Claims 1, 3-22, and 24-42 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In these claims applicants mention "obtaining information **at least nearly unique** to the computing device.....whereby the generated file names and corresponding paths are likewise **at least nearly unique** to the computing device" which is generally narrative and indefinite with the invention. Applicants do not point out clearly which options include in the present invention by "**at least nearly unique**". The ambiguity of applicant's argument is very difficult to understand how this terms could be definite wherein he agreed that this is indefinite (in the argument, page 13), "....items be unique to the computing device **but not so unique** as to guarantee....." The office will interpret these words with the regarding claims as best understood for applying the appropriate art for rejection purposes. Applicant's amended part "**consistently obtainable**" is indefinite as well. Examiner could not understand the obtained information consistent with what? Is it consistent with the computing device or anything else?

Response to Arguments

7. Applicant's arguments with respect to claims 11, 3-22, and 24-42 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 3-22, and 24-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Jong et al hereafter Jong (US patent application 20050069138) in view of Johnson et al hereafter Johnson (US Patent application 20030163718).

9. As per claim 1, and 22 Jong discloses a method and a medium comprising: obtaining information at least nearly unique to the computing device, the obtained information being generally non-changing and consistently obtainable and being selected from a group consisting of a hardware identification (HWID) generated for the computing device based on one or more identifications of hardware of the computing device, and a specific time associated with the computing device (paragraphs, 0108-0109, and 0012). Although Jong mention about the memory location with has function

(paragraphs, 0119-0120, 0152, and 0168). He does not expressly mention determining a number x of locations at which at least a portion of the state store is to be stored at; generating x pseudo-random file names and x corresponding paths based at least in part on the obtained information by applying a one-way function to data including the obtained information and employing a resulting output of the function to define the file named and the paths, whereby the generated file names and corresponding paths are likewise at least nearly unique to the computing device; pairing the x generated file names and the x generated paths to form the x locations; and storing the state store according to the x generated locations. In the same field of endeavor Johnson discloses determining a number x of locations at which at least a portion of the state store is to be stored at; generating x pseudo-random file names and x corresponding paths based at least in part on the obtained information by applying a one-way function to data including the obtained information and employing a resulting output of the function to define the file named and the paths, whereby the generated file names and corresponding paths are likewise at least nearly unique to the computing device; pairing the x generated file names and the x generated paths to form the x locations; and storing the state store according to the x generated locations (paragraphs 0020-0023, and 0043-0046).

Accordingly, it would been obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Johnson's teachings of stored locations for state with the teachings of Jong, for the purpose of suitably using the

hardware id for storing the sate store in the obfuscation application (paragraphs 0020-0023, and 0043-0046).

10. As per claim 3, Jong discloses the method comprising obtaining information specific to the computing device comprising an install time of an operating system thereof (paragraphs, 0108-0109, and 0012).

11. As per claim 4, Jong discloses the method comprising obtaining information specific to a current period of time, whereby the state store is stored according to a location that varies according to such current period of time (paragraphs, 0119-0120, 0152, and 0168).

12. As per claim 5, Jong does not disclose the method comprising determining the number x of locations as a number n of parts in which the state store is to be divided times a number m of copies of each part that are to be stored. However, Johnson disclose determining the number x of locations as a number n of parts in which the state store is to be divided times a number m of copies of each part that are to be stored (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 5.

13. As per claim 6, and 7 Jong does not disclose the method comprising generating x pseudo-random file names, each having a pseudo-random name length, generating x paths, each path comprising one of a plurality of levels of an operating system directory path on the computing device. However, Johnson disclose generating x pseudo-random file names, each having a pseudo-random name length, generating x paths, each path

comprising one of a plurality of levels of an operating system directory path on the computing device (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 6, and 7.

14. As per claim 8, and 9 Jong does not disclose the method comprising generating x paths, each path comprising one of a plurality of levels of a registry path on the computing device, wherein storing the state store according to the x generated locations comprises: protecting the state store by performing at least one of: signing the state store to produce a signature and appending the signature to the state store; and encrypting the state store to produce an encrypted state store; dividing the state store into n parts; saving each of the n parts m times according to the x = n times m formed locations. However, Johnson disclose generating x paths, each path comprising one of a plurality of levels of a registry path on the computing device, wherein storing the state store according to the x generated locations comprises: protecting the state store by performing at least one of: signing the state store to produce a signature and appending the signature to the state store; and encrypting the state store to produce an encrypted state store; dividing the state store into n parts; saving each of the n parts m times according to the x = n times m formed locations (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 8, and 9.

15. As per claim 10, and 11 Jong disclose obtaining the information at least nearly unique to the computing device (paragraphs, 0108-0109, and 0012). He does not expressly disclose the method wherein storing the state store according to the x generated locations comprises: dividing the state store into n parts; protecting the state store by signing at least one of the n parts of the state store to produce a signature and appending the signature to the part; and saving each of the n parts according to the x formed locations, retrieving the stored state store, the retrieving comprising: determining the number x of locations at which at least a portion of the state store is stored at; generating the x pseudo-random file names and the x corresponding paths based at least in part on the obtained information; pairing the x generated file names and the x generated paths to form the x locations; and retrieving the state store from the x generated locations. However, Johnson disclose storing the state store according to the x generated locations comprises: dividing the state store into n parts; protecting the state store by signing at least one of the n parts of the state store to produce a signature and appending the signature to the part; and saving each of the n parts according to the x formed locations, retrieving the stored state store, the retrieving comprising: determining the number x of locations at which at least a portion of the state store is stored at; generating the x pseudo-random file names and the x corresponding paths based at least in part on the obtained information; pairing the x generated file names and the x generated paths to form the x locations; and retrieving the state store from the x generated locations (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 10, and 11.

16. As per claim 12, and 13 Jong does not disclose the method wherein the state store has been divided into n parts and each of the n parts has been saved according to the x formed locations, and wherein retrieving the stored state further comprises: retrieving the n parts from the x locations; reconstituting the state store from the retrieved n parts thereof; if the reconstituted state store is encrypted, decrypting same; and if the reconstituted state store is signed to produce a signature, verifying the signature, wherein the state store has been divided into n parts and each of the n parts has been saved m times according to the x formed locations, and wherein retrieving the stored state comprises reconstituting m copies of the state store from the retrieved n parts thereof, and further comprises randomly selecting one of the m reconstituted copies. However, Johnson discloses the method wherein the state store has been divided into n parts and each of the n parts has been saved according to the x formed locations, and wherein retrieving the stored state further comprises: retrieving the n parts from the x locations; reconstituting the state store from the retrieved n parts thereof; if the reconstituted state store is encrypted, decrypting same; and if the reconstituted state store is signed to produce a signature, verifying the signature, wherein the state store has been divided into n parts and each of the n parts has been saved m times according to the x formed locations, and wherein retrieving the stored state comprises reconstituting m copies of the state store from the retrieved n parts

thereof, and further comprises randomly selecting one of the m reconstituted copies (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 12, and 13.

17. As per claim 14, and 15 Jong does not disclose the method comprises: hashing data including the obtained information to produce a first hash comprising a string of numbers; for each file name length, applying a pre-defined serial portion of the first hash to a function to result in the file name length; and for each Nth file name: performing a predetermined modification to the Nth hash; hashing the modified Nth hash to produce an (N+l)th hash comprising a string of numbers, whereby the first hash is employed to produce a second hash for the first file name, the second hash is employed to produce a third hash for the second name, etc.; and for each file name character of the Nth file name, applying a pre-defined serial portion of the (N+l)th hash to a function to result in the file name character, wherein each file name length has a preset minimum and maximum, and wherein applying the pre-defined serial portion of the first hash to a function to result in the file name length comprises applying the pre-defined serial portion of the first hash to the modulo function: Length = [serial portion mod (maximum - minimum)] +minimum. However, Johnson discloses hashing data including the obtained information to produce a first hash comprising a string of numbers; for each file name length, applying a pre-defined serial portion of the first hash to a function to result in the file name length; and for each Nth file name: performing a predetermined modification to the Nth hash; hashing the modified Nth hash to produce an (N+l)th hash

comprising a string of numbers, whereby the first hash is employed to produce a second hash for the first file name, the second hash is employed to produce a third hash for the second name, etc.; and for each file name character of the Nth file name, applying a pre-defined serial portion of the (N+I)th hash to a function to result in the file name character, wherein each file name length has a preset minimum and maximum, and wherein applying the pre-defined serial portion of the first hash to a function to result in the file name length comprises applying the pre-defined serial portion of the first hash to the modulo function: Length = [serial portion mod (maximum - minimum)] +minimum (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 14, and 15.

18. As per claim 16, 17 and 18 Jong does not disclose the method wherein applying the pre-defined serial portion of the (N+I)th hash to a function to result in the file name character comprises applying the pre-defined serial portion of the first hash to a conversion table predefined for the computing device, wherein the modification comprises at least one of a bit shift, a reverse ordering, and a swapping, wherein each path comprises one of a plurality of levels of an operating system directory path on the computing device, and wherein generating x paths based at least in part on the obtained information comprises: hashing data including or based on the obtained information to produce a path hash comprising a string of numbers; for each path, applying a pre-defined serial portion of the path hash to a function to result in a level for the path. However, Johnson discloses wherein applying the pre-defined serial portion of

the (N+I)th hash to a function to result in the file name character comprises applying the pre-defined serial portion of the first hash to a conversion table predefined for the computing device, wherein the modification comprises at least one of a bit shift, a reverse ordering, and a swapping, wherein each path comprises one of a plurality of levels of an operating system directory path on the computing device, and wherein generating x paths based at least in part on the obtained information comprises: hashing data including or based on the obtained information to produce a path hash comprising a string of numbers; for each path, applying a pre-defined serial portion of the path hash to a function to result in a level for the path (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 16, 17 and 18.

19. As per claim 19, and 20 Jong does not disclose the method wherein each path level has a preset minimum and maximum, and wherein applying the pre-defined serial portion of the path hash to a function to result in the level for the path comprises applying the pre-defined serial portion of the path hash to the modulo function: Level = [serial portion value mod (maximum - minimum)] +minimum, defining successive periods of time, and for each successive period of time: obtaining information at least nearly unique to the computing device; determining a number x of locations at which at least a portion of the state store is to be stored at; generating x pseudo-random file names and x corresponding paths based at least in part on the obtained information and based at least in part on indicia relevant to the period of time, whereby the generated

file names and corresponding paths are likewise at least nearly unique to the computing device and unique to the period of time; pairing the x generated file names and the x generated paths to form the x locations; and storing the state store according to the x generated locations, whereby the state store is moved during each successive period of time. However, Johnson discloses wherein each path level has a preset minimum and maximum, and wherein applying the pre-defined serial portion of the path hash to a function to result in the level for the path comprises applying the pre-defined serial portion of the path hash to the modulo function: Level = [serial portion value mod (maximum - minimum)] +minimum, defining successive periods of time, and for each successive period of time: obtaining information at least nearly unique to the computing device; determining a number x of locations at which at least a portion of the state store is to be stored at; generating x pseudo-random file names and x corresponding paths based at least in part on the obtained information and based at least in part on indicia relevant to the period of time, whereby the generated file names and corresponding paths are likewise at least nearly unique to the computing device and unique to the period of time; pairing the x generated file names and the x generated paths to form the x locations; and storing the state store according to the x generated locations, whereby the state store is moved during each successive period of time (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 19, and 20.

20. As per claim 21 Jong discloses the method comprising: obtaining alternate information relevant to the computing device (paragraphs, 0108-0109, and 0012). He does not expressly discloses generating at least one pseudo-random file name and at least one corresponding path based at least in part on the alternate information and pairing same to form at least one alternate location; and storing the obtained information as original information according to the at least one generated alternate location, whereby if the obtained information changes on the computing device, such changed information cannot be employed to retrieve the state store but the alternate information can be employed to retrieve the original information and the original information can be employed to retrieve the state store. However, Johnson discloses generating at least one pseudo-random file name and at least one corresponding path based at least in part on the alternate information and pairing same to form at least one alternate location; and storing the obtained information as original information according to the at least one generated alternate location, whereby if the obtained information changes on the computing device, such changed information cannot be employed to retrieve the state store but the alternate information can be employed to retrieve the original information and the original information can be employed to retrieve the state store (paragraphs 0020-0023, and 0043-0046).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 21.

21. Claims 10-15 are listed all the same elements of claim 2-7 but in computer system form rather than device form. Therefore, the supporting rationales of the rejection to claim 2-7 apply equally as well to claim 10-15.

Conclusion

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **MOAZZAMI NASSER G** can be reached on **(571)272-4195**. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/7/07